

TERM OF REFERENCE

PROVISION OF THE ONLINE INDUSTRY PLATFORM SYSTEM FOR INDUSTRY COLLABORATION PROGRAM (ICP) 2.0, CYBERSECURITY MALAYSIA

1 BACKGROUND

- 1.1. CyberSecurity Malaysia (CSM) has successfully published its first printed copy of the Cyber Security Industry Directory (CID) in 2013 (CID 2013). CID is aimed to be an industry reference for the local industry. A concise and comprehensive directory listing allow those working in the industry to connect and promote their products and services amongst peers and cross-industries through conventional medium. It also serves as a basic platform in bringing together common industry players.
- 1.2. Following that, CID 2013 has been reviewed and updated accordingly of which the number of companies included under CID 2014 has increased from 173 to 250.
- 1.3. As part of an Industry Collaboration Program (ICP) initiative, it is timely for CSM to embark into further developing and creating the right online platform in bringing the government and industry together as a means of creating competitive advantage to the local players and also increase the economic contribution of cyber security industry to the nation.
- 1.4. **Figure 1** illustrates the existing (CID) and new platform (ICP) capabilities and system feature requirements.

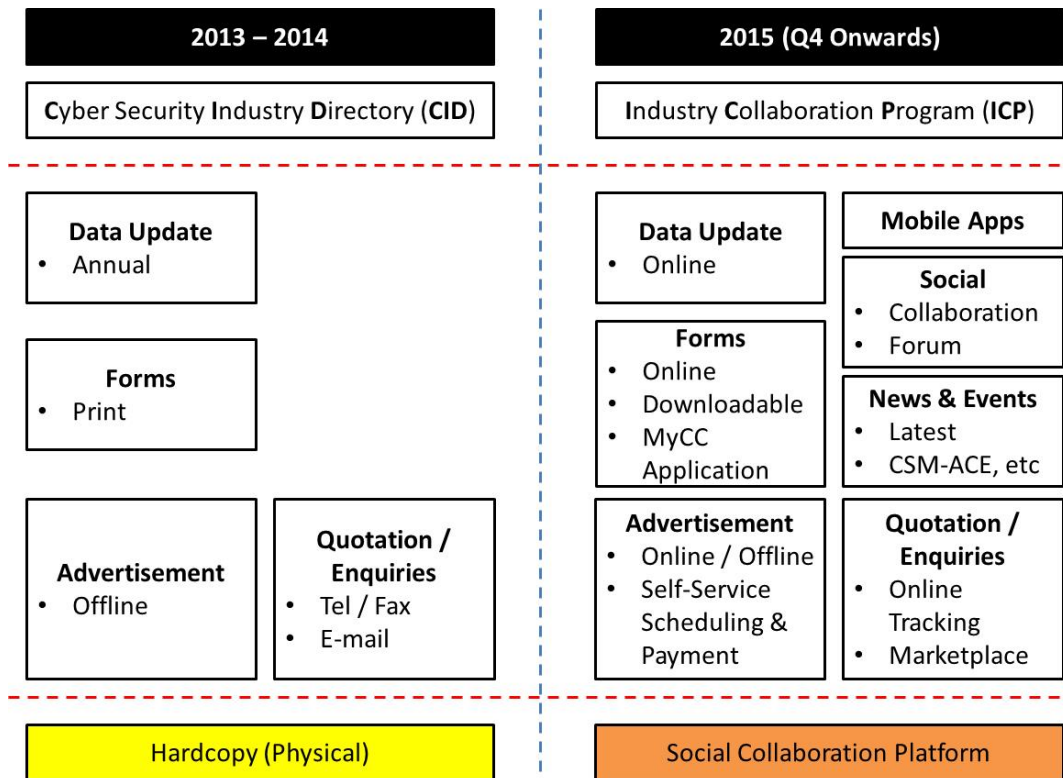


Figure 1: Existing (CID) and new platform (ICP) capabilities and system features

2 OBJECTIVE

The objective of the online industry platform is to allow access for the local cyber security industry players (ICP members and non-members) to socially collaborate, network, share knowledge as well as facilitate marketing of locally developed products and/or services within its own community and beyond.

3 REQUIREMENTSDESCRIPTION

As illustrated in **Figure 1**, the initial requirement for the online industry platform came from the need to have an online version of the latest CID. Thus, the basic functionalities of the online industry platform include proper storage and update of local companies involved in cyber security using a database; simple and advance directory listing with sort and search feature; as well as advertisement space for products/services.

However, with an online system in place, the investment should be optimized by leveraging other available system capabilities and features in-line with current industry needs and trends.

With the objective of the online industry platform in mind, the ICP social collaboration platform system specifications shall have the following four main criteria to cater for the current requirements and future expansions:

- a. Social platform;
- b. Content Management System (CMS);
- c. Mobile apps-ready; and
- d. Open source with support option.

Therefore, at the minimum, the bidder shall propose a suitable platform solution (hardware and software) to support the following capabilities and features:

3.1 Data Update

Local cyber security industry players must be able to register their companies via online application. Once the application has been reviewed and approved, the company shall be included in the industry directory listing.

3.2 Forms

Physical paper application forms such as ICP member application form, event participation form, and MyCC developer application form shall be converted into online application forms and linked to the database. Once visitor enters registration details and submit the application, the details must be captured and stored accordingly in the database for further processing.

At the same time, these forms shall also be converted into PDF format and made available for download at respective pages.

3.3 Advertisement

Advertisement slot(s) with various predetermined sizes are made available for purchase on the social collaboration platform. Advertisers can choose whether to advertise their company, products and/or services online (on the social collaboration platform), offline (CID printed hardcopy) or both.

Advertisers can apply for the advertisement slot(s) and select their desired schedule(s) such as advertise for a duration of one-month prior to an event. Once satisfied, the advertiser can then make online payment based on advertisement pricing scheme.

3.4 Social Platform

Registered members with proper online credentials can submit and share their contents on the social collaboration platform. The contents shall be published once reviewed and approved.

The forum shall allow registered members to contribute and collaboratively share their ideas. Visitors are allowed to view the forum contents, but can only post a reply after registering as a member.

Member registration and login credentials shall be tied to other social media networks such as Facebook, LinkedIn, and Twitter. With this integration, members will be able to follow, connect and interact with other members in a familiar social environment.

3.5 News & Events

Latest news related to cyber security either local, regional or global are regularly updated and displayed on the social collaboration platform.

The same applies to listing of local and regional cyber security related events.

3.6 Quotation / Enquiries

Visitors, members and/or potential customers can make enquiries for products and/or services offered by the local industry.

Enquiries can be answered by any of the registered companies. However, request for quotations can only be replied by selected members such as ICP member companies.

The enquiries and quotation requests shall be tracked online by CSM.

At the same time, the social collaboration platform must have the capabilities to the host ICP marketplace to promote locally developed and certified cyber security products / services.

3.7 Mobile Apps-Ready

The proposed social collaboration platform must be mobile apps-ready to facilitate the development of mobile apps at a later stage in the near future. The online industry platform can be accessed and used through the plethora of modern devices such as smartphones and tablets and the mobile apps be made available on Google Play, App Store, Windows Store, and BlackBerry Store.

3.8 Search

Having a search box makes it easier for visitors to find content. It can also help CSM gather information about what visitors want to find and are coming to the site for, such as product information, keyword usage and visitor wants and needs.

The search box shall include what is searchable on the site, such as keywords or item numbers.

3.9 Sign In and Sign Up

Sign in page is linked with the database to authenticate registered social collaboration platform users. Users must sign in using their

email address as username along with eight-character alphanumeric password. Users have the option to select “Remember me”.

Should a user forget his/her login credentials, the user can click on “Forgot password?” link which allows the user to reset the password.

At the same time, new users can sign up by clicking “Sign Up” link. The user must then enter web registration details and the user information entered automatically stored in the database.

3.10 Content Management System (CMS)

With the various contents that shall be made available on the platform, CMS is necessary to facilitate publishing, editing and modifying of contents, organizing, deleting as well as maintenance from a central interface. Since the ICP platform is a collaborative environment, CMS shall provide the procedures to manage related workflows.

3.11 Scalable System

The online industry platform shall be scalable with the capability to handle the growing requirements such as but not limited to:

- Marketplace for ICP members' products and/or services
- Payment gateway integration

3.12 Non Functional Requirement

Non Functional Requirements and Method definition of security criteria of the system upon pre-development or during development process is described in Appendix 1 and Appendix 2

3.13 Figure 2 illustrates the design overview of the social collaboration platform.

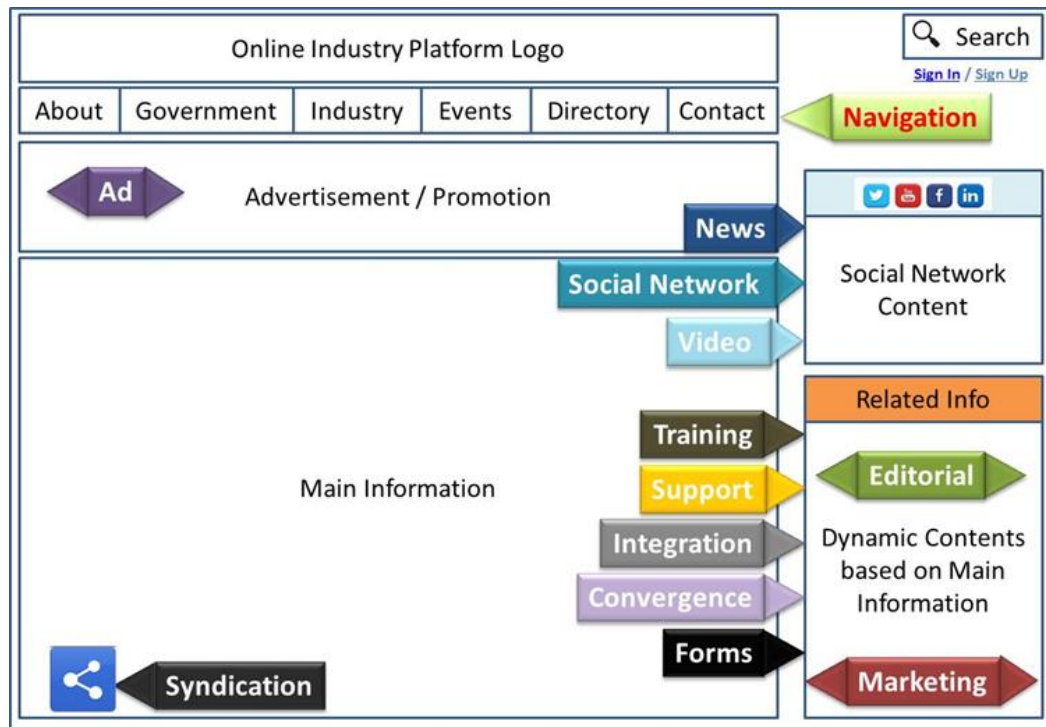


Figure 2: Design Overview of the Social Collaboration Platform

4 SCOPE OF WORK

The bidder is required to submit a proposal. The proposal shall include details such as:

- system architecture;
- hardware specifications;
- software capabilities and functionalities;
- disaster recovery; and
- project timeline.

The bidder must propose a suitable system to meet the objective of the online industry platform.

The proposed system for the online industry platform is recommended to include the following manner:

4.1 Phase1

Phase 1 primarily consists of delivery of the bidder's proposed system (hardware, software and licenses) for the online industry platform.

4.1.1 Hardware

The proposed system architecture can either be cloud-based or server-based. Regardless of the proposed platform, the bidder must provide a suitable hardware specification and the hardware is to be setup and configured accordingly and includes specifications and/or services such as:

- Dell, IBM or equivalent server
- Server RAID configuration
- Server delivery and mounting in rack (applicable for server-based system)
- Power, network, and/or KVM switch cabling (applicable for server-based system)
- ISO/IEC 27001:2013 certified (applicable for cloud-based system)
- For cloud based environment, the bidder to propose a secured cloud service provider which offer good services, reliable, 24/7 support, Data Recovery and backup.

4.1.2 Software and Licenses Installation and Configuration

Since the proposed system architecture can either be cloud-based or server-based, the bidder shall provide suitable software specifications that meet the described requirements along with the necessary licenses. The

software is to be setup and configured accordingly and includes specifications and/or services such as:

- Operating system, device drivers and licenses for 3-years
- Server hostname and IP address
- Database and license for 3-years
- Other related platforms and/or licenses (disaster recovery, virtualization, etc.) for 3-years
- Other software dependencies such as Java, Microsoft Dot Net, etc.

4.2 Phase 2

Phase 2 deliverables mainly include development and integration of proposed system as well as testing and commissioning.

4.2.1 Development & Integration

Integration of developed content into the bidder's proposed system for the online industry platform:

- Data extract, transfer and load (ETL) into the database (data such as industry directory which is currently available in Microsoft Excel format)
- Searchable content
- Sorting of retrieved/displayed information
- Content management
- Malaysian Common Criteria Evaluation & Certification (MyCC) online application
- Business intelligence (reporting, site statistics, etc.)

- Calendar reminder, Google Maps, etc.

4.2.2 Testing and Commissioning

Overall system testing and commissioning such as:

- Server hostname(s) and DNS configuration
- Firewall configuration
- Database and web server connection
- User Acceptance Test (UAT) plan
- System fine tuning
- Final testing and commissioning

4.2.3 Performance Requirement

- 100 % or 95% of the operation carried out in the system must respond within 5 seconds
- The system has to support 100 concurrent users
- The system capable to support 1000 customers and users when implemented into Production.

4.2.4 Mobile Apps Development

Development of mobile apps based on the social collaboration platform capabilities and features:

- Development of mobile apps for Android, iOS, Windows Phone, and BlackBerry OS
- Testing and Fine Tuning
- Commissioning of mobile apps Google Play, App Store, Windows Store, and BlackBerry Store

4.3 Phase 3

4.3.1 Maintenance and Support Services

Maintenance and support services including:

- Inclusive Warranty for six (6) months and quarterly preventive maintenance for three (3) years and support services. An example of support service include Return Merchandise Authorization (RMA) if the proposed system is server-based
- Platform patches, updates, and upgrades
- 24/7 e-mail and phone call support
- Remedial maintenance
- Search Engine Optimization (SEO)

5 PROJECT DELIVERABLES & TIMELINE

The Project should be successfully delivered not later than **7** (seven) months from the date the Project is awarded to the successful bidder with the following details:

	Activity	*Timeline
1.	Letter of Award (LoA) is issued by CyberSecurity Malaysia.	T1
2.	<u>Phase 1</u> • Hardware Setup and Configuration • Software and Licenses Installation and Configuration	T2=T1+ 2w
3.	<u>Phase 2</u> • Development & Integration Services • Testing and Commissioning	T3=T2+6m

	Activity	*Timeline
	Mobile Apps Development	
4.	<u>Phase 3</u> Maintenance and Support Services	After T3

** Timeline by which activities shall be completed ('T1' is the date of the LoA issuance. 'w' means time period of a week and 'm' means time period of a month)*

6 PROJECT MANAGEMENT APPROACH

6.1 The successful bidder must engage with the appointed SME for the Development of Industry Collaboration Program (ICP) 2.0.

6.2 The bidder shall provide the documentation below for the project implementation:

6.2.1 User Requirement Document

6.2.2 Project Progress Meeting Documentation, including Minutes of Meeting and Slides presentation

6.2.3 User Acceptance Test (UAT) approved by both parties.

6.2.4 System design document

6.2.5 User manual

7 BIDDER RESPONSIBILITY

7.1 The Bidder is subjected to all existing government guidelines, procedures and regulations pertaining to the procurement and the conduct of the professional services.

7.2 The Bidder shall confirm that their proposal is based on the entire provision of the above scope of works/terms of reference. The

Bidder's partial compliance with the said scope of works/terms of reference shall be disqualified.

- 7.3 The provision for a three (3) year standard hardware warranty services from the date of commissioning and acceptance by CyberSecurity Malaysia. Thus, the Bidder must provide details on the above warranty services in their bid proposal.
- 7.4 The bidder shall review this document and take full responsibility for obtaining the necessary information from CyberSecurity Malaysia as may be required to meet the specifications and requirements.
- 7.5 The bidder shall review and fulfil all specifications and requirements before committing to sign the purchase agreement.
- 7.6 CyberSecurity Malaysia reserves the right to reproduce all or part of the document submitted by the bidder for internal use.

8 POINT OF CONTACT

- 8.1 The Bidder shall nominate an executive within its organization, whom shall be a full-time employee of the organization to be the working together with the Project Owner from CSM. The appointed person shall be the single point of contact between the Bidder and CSM.

--- END OF DOCUMENT---

APPENDIX 1**Non-Functional Requirement****1. Operating System**

1.1. Require latest operating system from UNIX / Windows.

2. User Acceptance Test

- 2.1. UAT exercise done and involved CyberSecurity Malaysia's representative and vendor.
- 2.2. UAT result documented and approved by both parties.

3. Security

The portal must be tested with the Vulnerability Audit Assessment conducted by CyberSecurity Malaysia after User Acceptance Test (UAT) exercise.

3.1. The Vulnerability Audit Assessment should cover but not limited to below criteria:

- 3.1.1. Injection
- 3.1.2. Broken Authentication and Session Management
- 3.1.3. Cross-Site Scripting (XSS)
- 3.1.4. Insecure Direct Object References
- 3.1.5. Security Misconfiguration
- 3.1.6. Sensitive Data Exposure
- 3.1.7. Missing Function Level Access Control
- 3.1.8. Cross-Site Request Forgery (CSRF)
- 3.1.9. Using Known Vulnerable Components
- 3.1.10. Unvalidated Redirects and Forwards
- 3.1.11. Input Data Validation

For more detail about criteria, please refer to Appendix 2.

- 3.2. The portal must be equipped with timeout session management for users (recommended - 15 minutes).
- 3.3. Session management for portal must only allow single session at one time.
- 3.4. The portal MUST use secure protocols (e.g., SSL).
- 3.5. All Operating System based in server must be installed with latest Anti-Virus version.
- 3.6. Source code shall not reveal any confidential information.
- 3.7. User access privileges have to be spelled out and well documented.

4. Log

- 4.1. The portal **MUST** be able to generate log for audit purposes (e.g. activity logs for admin and user).
- 4.2. Ensure that log files were stored in a location with adequate size spaces, log files should be partitioned separately.

5. Maintenance

- 5.1. Automatic updates for the portal and its Operating system **MUST** be enabled (as define by CyberSecurity Malaysia).
- 5.2. The portal **MUST** be able to provide backup function.
- 5.3. The portal must include with a warranty (6months) and quarterly preventive maintenance within 3 years.
- 5.4. Source code shall belong to CyberSecurity Malaysia (applicable only for a new system that has been developed on full SDLC methodology).
- 5.5. The portal must be scalable for future enhancement.

APPENDIX 2

Method definition for security criteria of system upon pre-development or during development process

No	Method	Description
1.	Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when a trusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.
2.	Broken Authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing Attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities.
3.	Cross-Site Scripting (XSS)	XSS flaws occur whenever an application takes entrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
4.	Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
5.	Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date.
6.	Sensitive Data Exposure	Many web applications do not properly protect sensitive data, such as credit cards, tax ids, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes. Sensitive data deserve extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
7.	Missing Function Level Access Control	Virtually all web applications verify function level access rights before making that functionality visible in the UI.

		However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access unauthorized functionality.
8.	Cross-Site Request Forgery (CSRF)	A C5RF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim .
9.	Using Components with Known Vulnerabilities	Vulnerable components, such as libraries, frameworks, and other software modules almost always run with full privileges. So, if exploited, they can cause serious data loss or server takeover. Applications using these vulnerable components may undermine their defenses and enable a range of possible attacks and impacts.
10.	Un-validated Redirects and Forwards	Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware site, or use forwards to access unauthorized pages.
11.	Input Data Validation	Each Web application input data from HTTP requests must be checked against a strict format that specifies exactly what input will be allowed. All headers, cookies, query strings, form fields, and hidden fields (i.e., all parameters) must be "positively" validated against a rigorous specification that defines: i. Data type (string, integer, real, etc.) ii. Allowed character set iii. Minimum and maximum length iv. Whether null is allowed v. Whether the parameter is required or not vi. Whether duplicates are allowed vii. Numeric range viii. Specific legal values (enumeration) and specific patterns (regular expressions)